Luna securităţii cibernetice

Proiect realizat de:

Ceban Anamaria

Bujor Claudiu

Profesor:

Guţu Maria

SLIDE. 1 (Introducere)

Astăzi vom vorbi şi vom învăţa câte ceva despre securitatea cibernetică si cea de pe internet.

Drept citat pentru această lecţie am ales citatul: (**Stop-Think-Connect**). Ce ar putea semnifica acest citat in câteva cuvinte? Păi, noi l-am descifrat astfel... (Atunci când navighezi pe internet, nu te grăbi să faci lucruri nechibzuite, iar dacă nu esti destul de sigur în ceea ce faci, mai bine gândeştete de două ori înainte de a acţiona, iar în cazuri problematice, rugaţi ajutorul unei persoane cu cunostinţe mai aprofundate în acest domeniu).

SLIDE. 2 (Internetul)

În continuare vom vorbi despre internet în linii generale. CE , CÂND şi CUM a apărut acesta.

--„„Apropo, cine din voi cunoaşte când a apărut internetul de care ne folosim noi astăzi ?””

Internetul, dar mai exact termenul de internet a apărut în anul **1974.** De ce am spus (mai exact termenul de internet), păi din cauza că, de fapt, internetul şi-a început existenţa înca de prin anii **50’**. Haideţi să va spun in câteva cuvinte cum a ajuns la ceea ce este el astăzi. Deci cum am mai

spus, internetul şi-a inceput primele apariţii incă de prin anii **50'**. De la începu acesta a fost considerat si folosit ca armă de către USA împotriva U.R.S.S. Pe atunci oamenii de ştiinţă îl foloseau ani întregi pentru a face schimb de informaţie între ei în timpul Războiului Rece. În anul **1962** omul de stiinţă american **J.C.R. Licklider** a propus ideea pentru o reţea de calculatoare care vor putea comunica unul cu altul. În anul **1969** a fost trimis primul mesaj de la un calculator la altul prin reţeaua americană **ARPANET (Agenţia Avansată de Proiecte de Cercetare).** Din anul 1971 această reţea s-a extins tot mai mult în întreaga lume, în acest an fiind adaugată reţeaua **ALOHANET** din **Hawaii**, urmată de cîteva universităţi din **Anglia** şi **Norvegia 2 ani** mai târziu. Tot in acest an **Ray Tomlinson** se ocupă de crearea unui sistem care sa trimită mail-uri înainte şi înapoi între utilizatorii reţelei **ARPANET**. Mesajele se vor numi eventual mailuri electronice sau **E-mailuri**, după cum la cunoaştem noi azi. Odată cu creşterea numărului de calculatoare din reţea, a devenit tot mai dificil integrarea unei singure reţea la nivel mondial. Astfel în jurul anului **1980** este inventată **adresa IP**: funcţia acesteia era de a permite tuturor calculatoarelor din întreaga lume să comunice între ele într-un spaţiu virtual. Până în anul **1991** internetul era folosit de guvern, oameni de ştiinţă şi alte persoane importante, pentru transferul rapid de informaţii si fişiere. Însă în anul **1991** internetul suferă o schimbare importantă. Un programator elveţian numit **Tim Berners-Lee crează (World Wide Web)** prescurtat **(WWW).** Care poate fi descris drept o pânză de păianjen plină de informaţii care pot fi accesate de oricine are o conecţiune la internet. Iată cum a apărut internetul pe care îl folosim noi astăzi.

SLIDE. 3, 4, 5 (10 reguli)

În continuare vom reveni la discuţia noastră despre securitatea pe internet.

Iată 10 reguli pentru o navigare sigura pe internet:

…

Slide 4. Poza 3. Fiecare măcar odată, aţi văzut această fereastră atunci când aţi instalat un program pe calculator. Pentru cei ce nu ştiu atunci

când descarci un program pe calculator, prima fereastră care îţi apare este aceasta, unde eşti întrebat daca continui sau nu descărcarea. Uitându-ne la această fereastra, ni s-ar părea ca totul este în regulă, dar dacă privim mai atent putem vedea că cel care a editat acest program nu are un nume verificat. Asta ne duce la gândul că programul nu e licenziat, drept urmare nu este sigur si poate conţine fişiere virusate. De aceea când vedeţi aşa o fereastra de program, fără un nume de editor, să ştiţi că e mai bine să nu continuaţi descărcarea şi să căutaţi altă sursă. Dar cel mai bine desigur este, dacă aveţi posibilitatea, să cumpăraţi un program licenziat.

SLIDE. 6 ,7 (Cyber-bullying)

Hărţuirea online sau Cyber-bullying este termenul folosit pentru definirea diverselor forme de abuz psihologic pe internet: hărţuire, ameninţare, intimidare, adresare de injurii, transmiterea de mesaje obscene, uneori ajungându-se chiar şi la şantaj), cu scopul de a ataca o persoană.

În cazul în care sunteţi victime ale hărtuirii online, blocaţi si raportaţi acele persoane care vă fac rău sau dacă cineva a postat fără acordul tău poze cu tine sau informaţie personală, de asemenea te sfătuim să raportezi acest fapt administratorului site-ului pentru ca postarea să fie ştearsă. Te poţi adresa oricărei unităţi de poliţie pentru investigaţii, atunci când consideri că s-a adus atingere bunei reputaţii prin publicarea fără acord.

Dar pentru ca să evitaţi astfel de întâmplări trebuie să aveţi grijă de reputaţia voastră online.

SLIDE. 8 (Reputaţia online)

Ce înseamnă o reputaţie online?. Mulţi oameni încă nici nu înţeleg această noţiune, dar de ce aceasta este defapt atât de imprtantă?...

Conceptul de management al reputaţiei online este relativ nou, motiv pentru care multe persoane (printre care şi fondatori) nu acorda importanţă- incă- propriei imagini publice de care sunt urmăriţi pe web. Practic managementul reputaţiei online constă în acţiuni de

monitorizare, diminuare sau eliminare a materialelor negative pe care oamenii le găsesc despre sine online.

Iată niște pași pe care i-ai putea urmări în formarea propriei reputații online:

1. **Fă o căutare pe numele tău:**

--„„Cine dintre voi a încercat măcar o dată să-și caute numele pe google?””

Dacă nu atunci, încercați! Verificați atât rezultatele din search, cât și din google imagini.

De ce e important acest pas ?

--„„Vă voi da un exemplu concret””

Se cunoste cazul unui om pe nume Pete Kistler. Prin 2008 acesta a descoperit adevăratul motiv pentru care companiile la care acesta a aplicat nu îl chemau la nici măcar un interviu. Se pare că pe google existau mai mulți alți Pete Kistler, printre care se numără și un individ suspectat de trafic de droguri. Astfel observăm impactul reputației potențialilor angajați asupra angajatorului. Pentru a preveni astfel de situații, se recomanda să îți setezi alerte google pentru numele tău, adresa, numele bussiness-ului/brandului tău și să limitezi notificarea la una pe zi pentru a le primi direct pe email.

2. **Fii prezent activ pe rețelele de socializare:**

Când vorbim despre reputație online, vorbim totodata și despre rețelele de socializare. După cum bine știți acestea au devenit un canal de informare important, iar oamenii sunt foarte deschiși să își exprime părerile personale despre orice, fie ele pozitive, fie negative (și știți bine căveștile proaste circulă mai repede).

Atât în procesul de construire cât și întreținere a reputației tale online, e indicat să îți creezi profiluri pe principalele platforme de social și să le populezi cu informații relevante despre tine.

3. **Ține lucrurile private în privat, ai grijă ce postezi:**

Cu toții știm că ce se întâmplă pe google, rămâne acolo pentru totdeauna, și se va întoarce împotriva ta exact atunci când nu te vei aștepta. Prin urmare ai grijă ce publici online pentru că dacă tu nu ești

atent la propria reputaţie informaţiile negative se vor împrăştia ca gândul.

Există câteva reguli la prezenţa pe google, facebook sau orice alt website:

- Nu publica ceea ce nu vrei să vadă mama ta
- Nu publica ceea ce nu vrei să vadă şeful tău
- Şi nu publica orice-ţi trece prin cap

La fel stă treaba atât cu pozele necuvenite cât şi cu statusurile cu opinii personale discriminatorii, înjurioase sau care ar putea jigni pe cineva. **Nu au ce căuta online!**

- **VIDEO 9-Reputaţia online**

(Întrebări despre ce au reţinut…)

SLIDE. 10 (Cum depistăm un calculator virusat?)

Acum ca am vorbit si despre reputatia voastra online, putem trece şi la securitatea voastră online.

Cu toţii cunoaşteţi probabil câte ceva despre viruşi si că aceştia infectează deseori calculatoarele provocând daune, dar nu foarte mulţi ştiu cum se depistează un calculator virusat. Dacă aţi spus careva dintre frazele următoare ar fi bine să vă verificaţi calculatorul pentru viruşi.

1. "Computerul vorbeşte cu mine"

Adică pe ecran apar tot felul de ferestre pop-up şi mesaje publicitare care susţin că calculatorul vostru este infectata şi are nevoie de protecţie. Aici este vorba de un program spion (definiţie la care vom reveni).

2. "Computerul meu functioneaza extrem de incet"

Acesta poate fi un simptom pentru multe cauze, inclusiv infectarea cu un virus. În cazul în care s-a produs infectarea cu un virus, vierme sau troian, acestea pot consuma resursele calculatorului, făcându-l să funcţioneze mai greu decât de obicei.

3. "Am aplicaţii care nu pornesc"

De câte ori aţi încercat să porniţi o aplicaţie din meniul start sau de pe desktop si nimic nu se întâmpla? Uneori se poate deschide chiar un alt program. Ca şi în cazul anterior, poate fi vorba de orice altă problemă, însă este cel puţin un simptom care va spune că ceva nu este în regulă.

4. "Nu ma pot conecta la Internet sau acesta ruleaza extrem de incet"

Pierderea accesului la Internet este un alt semn al infectarii, desi poate fi cauzat si de probleme legate de router.

5. "Cand ma conectez la Internet, mi se deschid pe ecran tot felul de ferestre sau pagini web nesolicitate"

Acesta este cu siguranta un alt semn al infectarii calculatorului vostru. Multe fisiere virale (viruşi) sunt concepute special pentru redirectarea traficului de Internet catre anumite website-uri. Adică să deschidă o multime de site-uri fara voia voastră - a utilizatorului - atunci când va conectati la internet.

6. "Unde au disparut fisierele mele?"

Sa speram ca nimeni nu și-a pus această întrebare, desi anumite atacuri sunt concepute/făcute special pentru criptarea sau stergerea anumitor fisiere si chiar mutarea documentelor dintr-un loc in altul.

7. "Computerul meu, practic, a innebunit"

In cazul in care computerul dumneavoastra incepe sa actioneze singur sau sa trimita email-uri fara sa stiti, daca aplicatii sau ferestre de Internet se deschid singure sistemul sigur este compromis.

SLIDE. 11 (Malware)

Acum ca am depistat virusul, trebuie sa facem cunostinta cu el, nu?

Cuvantul virus, in sensul in care il folosim noi zi de zi nu inseamna altceva decât malware. Viruşii sau Malware esenţial sunt nişte soft-uri create pentru a dăuna sistemului, sterge date sau spiona activitatea voastră.

În continuare vom vorbi despre tipurile de malware cu care va puteti întâlni daca aveti ghinion.)

SLIDE. 12 (Virusi, Viermi si troieni)

1. **Viruşii (Slide 13)**

Un virus de calculator este un program care pentru voi ar arata ca unul obisnuit, insa acesta are capacitatea de a se multiplica, de a infecta diverse fisiere de pe computer, de a sterge informatii, etc. Viruşii se transmit de la un

calculator la alt calculator prin intermediul mediilor de stocare mobile, adica stick-urile sau floppy disck-ul, ori prin intermediul internetului.

Practic un virus este un program care va acţiona conform instrucţiunilor inserate în cod. Unii viruşi, de exemplu, infectează fişierele Word, cu care majoritatea dintre noi lucrează. După ce infectează un fişier Word, virusul ajunge pe alt calculator prin intermediul acestui fişier, care poate fi folosit de mai multe persoane pe mai multe calculatoare. De regulă, cu cât descoperim mai târziu un virus, cu atât dimensiunile stricăciunilor produse de acesta sunt mai mari.

2. Viermii (Slide 14)

Viermii sunt viruşi care nu infectează alte fişiere, ci doar se multiplică. Aceştia crează un singur exemplar, care caută metode de a se răspândi pe alte computere. Metodele "preferate" de răspândire sunt: emailul, aplicaţii tip "messenger" ori aplicaţiile de partajare de fişiere, gen torrents, emule, kazaa etc. Un vierme infectează sistemul informatic, nu fişierele.

3. Troieni (Slide 15)

Programele nocive tip "troian" sunt aplicaţii care sunt instalate fără ştiinţa şi acordul utilizatorului şi care efectuează diferite sarcini, ca de exemplu furtul parolelor, al diferitelor coduri prezente pe calculator, distribuirea necontrolată de emailuri, înregistrarea activităţilor desfăşurate pe calculator de către utilizator

etc. Troienii, spre deosebire de viruşi ori viermi, nu se pot răspândi singuri.

Troienii pot fi clasificaţi în:
::: backdoors - programe care odată instalate asigură o cale de comunicare secretă între computerul infectat şi realizatorul troianului, permiţând controlul de la distanţă al calculatorului;

::: password stealers - programe care, aşa cum spune şi numele, au rolul de a înregistra parolele folosite de utilizatorului calculatorului infectat şi transmiterea acestora către hacker.

::: bombe logice: programe care execută operaţiuni periculoase în anumite condiţii.

SLIDE. 16 (Protectia antivirus)

oftware-ul antivirus este folosit în general pentru prevenirea și eliminarea viruşilor de computer, viermilor și cailor troieni. De asemenea, poate detecta și elimina adware, spyware și malware.

3 dintre cele mai bune ptograme antivirus gratuite:
Avast
Avira
Bitdefender

O parte din produsele antivirus conțin pe lângă protecția

antivirus și alte module precum antispam, firewall, control parental și lista poate continua.

SLIDE. 17 (Securitatea aplicațiilor software)

Mai departe vom vorbi despre securitatea aplicațiilor.

SOFTWARE-prin software se înțelege un sistem de programare pentru calculator încluzând procedurile lor de aplicare, un sistem furnizat odată cu calculatorul sau creat ulterior de utilizator.

Cum îți protejezi software-ul?

Cu toate că nu există un mod foarte eficient de ați proteja software-ul, pentru că e imposibil să îl protejezi 100%, e necesar să faci acești pași:

- Faceți o protecție foarte bună împotriva copierii (piratării).

Chiar și la cele mai mari si mai securizate companii cum sunt Microsoft, s.a. se găsesc copii piratate ale produselor lor, astfel tot ce pot ei să facă este de a complica puțin activitatea hackerilor de a pirata produsele acestora, sau de a crea copii cu licență falsă, însă cum am mai spus sa protejezi un software definitiv e imposibil.

- Creați o licență pentru produs care poate fi utilizată nu mai mult de două calculatoare, licența trebuie să fie sigură și să aibă un termen de valabilitate in dependență de cerințele utilizatorului.
- Creați o strategie de licență:

Ca de exemplu. Puteți să oferiți o versiune de testare doar a programului, pentru o perioada limitata de timp. Sau puteți oferi o licență pe care o vindeți în mod periodic (de exemplu lunar), sa vă taxați o singură dată.

SLIDE. 18 (Securitatea pe retelele wifi publice)

Indiferent de frecvența folosirii acestor rețele, trebuie să fim conștienți că, de cele mai multe ori, ele nu au fost gândite ca să protejeze utilizatorii împotriva interceptării traficului de pe dispozitivele contactate la rețelele wireless.

Tratează orice reţea necunoscută cu mare grijă
Dacă se poate, evită să intri prin Wi-Fi pe site-urile care necesită logare
Evită, pe cât posibil, reţelele care solicită acces la date personale pentru a putea naviga pe Internet
Atenţie la erorile de conectare afişate de către browser / dispozitiv.
Este foarte important să nu ignori aceste erori – există riscul ca cineva să încerce să îţi intercepteze traficul.

SLIDE. 19 (Spam-urile)

- **Unde se poziţionează spamul, în raport celelalte categorii de ameninţări informatice?**

E greu de stabilit exact care din ameninţările informatice sunt mai dăunătoare (luând aici în considerare spam-ul şi diversele tipuri de malware). Însă este o certitudine faptul că ele se ajută unele pe celelalte pentru a face un rău general mai mare calculatorului. E ca un lanţ.

De exemplu: un **vierme** (care este o forma de **malware**) poate aduce cu sine şi un **backdoor** care îi va permite să transforme sistemul utilizatatorului într-un **”calculatorzombie”** care va face parte dintr-un **botnet**, controlat de autorul viermelui. În felul acesta sistemul controlat va primi comenzi şi va trimite spam-uri la diverse adrese electonice (e-mailuri). Aceste spamuri la rândul lor pot să conţină fişiere infectate atașate, sau diferite linkuri de descărcare care dăunează.

În urmare...

- **Care sunt principalele canale de răspândire a mesajelor spam?**

Cu siguranţă că e-mailurile, pentru că majoritatea oamenilor deţin o adresă de e-mail, folosită fie în scop profesional, fie în scop personal.

Există şi spam în formă de comentarii pe diferite reţele de socializare şi diferite forum-uri însă ele sunt mai greu de depistat.

- **Cum te fereşti de spam?**

Utilizatorul trebuie să aibă un produs de securitate complet (antivirus de exemplu) care să conţină şi modul antispam, altfel acesta nu va fi niciodata protejat 100%.

SLIDE. 20 (Spyware)

Un alt pericol pentru calvulatoarele voastre este programul spyware sau spion (mentionat ma sus).

Programele spion sau spyware sunt o categorie de software rău intenţionat, ataşate de obicei la programe gratuite care captează pe ascuns date de marketing (prin analiza siturilor pe care le vizitează utilizatorul, de exemplu de modă, pantofi, cluburi de tenis, ş.a.m.d. şi le folosesc apoi pentru a transmite utilizatorului reclame corespunzătoare dar nesolicitate.
Programele spion care nu extrag date de marketing, ci doar transmit reclame se numesc adware .

SLIDE. 21 , 22 (Keyloggeri)

Un tip de spyware ar fi Keyloggerii.

Un keylogger este un program care înregistrează fiecare bătaie de tastă pe o tastatură şi salvează aceste date într-un fişier. După ce colectează o anumită cantitate de date, le va transfera prin intermediul internetului unei gazde de la distanţă, predeterminată. De asemenea, poate captura capturi de ecran şi utiliza alte tehnici pentru a urmări activitatea utilizatorului. Un keylogger

poate cauza pierderea parolelor, date de autentificare, şi alte informaţii similare.

SLIDE. 23 , 24 (Phishing)

Acum să ne intoarcem la emailurile suspicioase. Un tip de email care poate sau nu intra in lista voastra de Spam este emailul de tip phishing.

Phishingul este o metodă de înşelătorie aproape la fel de veche ca şi Internetul. Infractorii se folosesc de inginerii sociale pentru a păcăli utilizatorii, infectându-le computerele, furându-le banii sau chiar identitatea. Tentativele de phishing se bazează pe emailuri, mesaje instant sau chiar şi apeluri telefonice, şi încercă să îi convingă pe utilizatori să acceseze anumite site-uri sau să îţi dea anumite date personale. Site-urile respective sunt fie copii perfecte ale unor site-uri cunoscute (Facebook, site-uri ale unor bănci, PayPal), sunt fie infectate cu viruşi.

SLIDE. 25, 26 (Comunicarea pe reţelele de socializare)

- Plusurile unei reţelele de socializare:
  - ➢ Popularitatea
  - ➢ Legatura cu prietenii sau colegii de liceu/facultate
  - ➢ Să ne găsim o relaţie sau un job mai bun
  - ➢ Este mai uşor să cunoşti persoane
- Minusuri:
  - ➢ Există diferite persoane periculoase, cu intenţii rele pe reţelele de socializare
  - ➢ Poţi fi victima unor ameninţări, agresări, înjosiri online

➢ Reputația ta online poate fi distrusă

Iată niște recomandări pentru a putea evita să fii șantajat pe internet:

...

...

...

Și încă niște sfaturi generale pentru siguranța proprie:

...

...

- **<u>3 Video Final:</u> În continuare veți putea viziona niște clipuri video despre securitatea în rețelel de socializare.**